STIC Search Report
EIC 2100

USPTO

STIC Database Tracking Number: 108597

TO:	From:
James Seal **Location: ** **Art Unit : 2131** **Wednesday, November 19, 2003** **Case Serial Number: 09870584**	**David Holloway** **Location: EIC 2100** **PK2-4B30** **Phone: 308-7794** **david.holloway@uspto.gov**

Search Notes

Dear Examiner Seal,

Attached please find your search results for above-referenced case.
Please contact me if you have any questions or would like a re-focused search.

David

sira
Search and Information Resources Administration

```
Set     Items   Description
S1       2490   PUBLIC()KEY? ? OR KEYPAIR? OR PUBLICKEY?
S2         90   S1(3N)(SIGN OR SIGNS OR SIGNING OR SIGNED OR AGREEMENT? OR
               AGREE OR AGREE? ? OR RULE? OR VALIDAT? OR (LIMIT? OR CONTROL?-
               )()ACCESS?)
S3         80   S2 NOT PD=19940719:19970719
S4         60   S3 NOT PD=19970719:20000719
S5          3   S4 NOT PD=20000719:20031120
File 347:JAPIO Oct 1976-2003/Jul(Updated 031105)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200374
         (c) 2003  Thomson Derwent
```

5/5/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008212601 **Image available**
WPI Acc No: 1990-099602/199013
XRPX Acc No: N90-076973

Public key cryptography system - allows trusted member of group to provide individual secret keys to other members of group and group membership to be authenticated

Patent Assignee: NCR CORP (NATC); NCR INT INC (NATC)
Inventor: AUSTIN J R; AUSTIN J
Number of Countries: 010 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9002456	A	19900308	WO 89US3253	A	19890727	199013	B
US 4944007	A	19900724	US 89364949	A	19890612	199032	
AU 8940524	A	19900323				199033	
EP 400103	A	19901205	EP 89909280	A	19890727	199049	
JP 3505033	W	19911031	JP 89508653	A	19890727	199150	
EP 400103	B1	19930721	EP 89909280	A	19890727	199329	
			WO 89US3253	A	19890727		
DE 68907717	E	19930826	DE 607717	A	19890727	199335	
			EP 89909280	A	19890727		
			WO 89US3253	A	19890727		
CA 1321835	C	19930831	CA 607081	A	19890731	199341	

Priority Applications (No Type Date): US 89364949 A 19890612; GB 8819767 A 19880819
Cited Patents: 2.Jnl.Ref
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9002456	A	E	24		
Designated States (National): AU JP					
Designated States (Regional): CH DE FR GB NL					
EP 400103	A				
Designated States (Regional): CH DE FR GB LI NL					
EP 400103	B1	E	14	H04L-009/30	Based on patent WO 9002456
Designated States (Regional): CH DE FR GB LI NL					
DE 68907717	E			H04L-009/30	Based on patent EP 400103
					Based on patent WO 9002456
CA 1321835	C			H04L-009/30	

Abstract (Basic): WO 9002456 A

At the trusted processor, the public key (N,e) is generated, where N is the product of two prime numbers (P,Q) and e is a corresponding public key integer value. Third and fourth prime number (R,S) are selected, and two values Nmi, psi (Nmi) are sent to the requesting device. The first value Nmi equals NRS and the second value psi (Nmi) equals psi (N)(R-1)(S-1) where the symbol psi represents the number of integers less than N which are relatively prime to N.

At the requesting device, fifth and sixth prime numbers, T,W are selected (152), and third and fourth values Nm, dm are computer (154), where Nm equals Nmi.TU and dm equal 1 + K psi (Nm) where psi (Nm) = psi (Nmi). (T-1). (u-1) and k, dm are integers. Consequently, dm is adapted for use by the requesting device as the secret key counterpart of the public key value e relative to the modulus Mn.

ADVANTAGE - Any group member may be provided with secret key for deciphering or **signing** data and matching **public key** easily derived.

5/7

Title Terms: PUBLIC; KEY; SYSTEM; ALLOW; MEMBER; GROUP; INDIVIDUAL; SECRET; KEY; MEMBER; GROUP; GROUP; MEMBER; AUTHENTICITY
Derwent Class: W01
International Patent Class (Main): H04L-009/30
File Segment: EPI

5/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

007752198
WPI Acc No: 1989-017310/198903
XRPX Acc No: N89-013340
Authentication of cards with electronic memory - using three zone memory with only two zones being readable to implement two-layer validation process.
Patent Assignee: SCHLUMBERGER IND SA (SLMB)
Inventor: BARAKAI S
Number of Countries: 011 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 299826	A	19890118	EP 88401645	A	19880628	198903	B
FR 2618002	A	19890113				198910	
US 4910774	A	19900320	US 88216644	A	19880708	199017	

Priority Applications (No Type Date): FR 879794 A 19870710
Cited Patents: EP 147337; EP 30381; FR 2536928; US 4094462; US 4211919
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 299826	A	F	9		

Designated States (Regional): BE CH DE ES FR GB IT LI NL SE

Abstract (Basic): EP 299826 A
The card memory is divided into three zones (Z1,Z2,Z3) the first (Z1) being accessible for reading and containing signature (S) data obtained from secret data (D) recorded in the third zone (Z3) which is inaccessible for reading. The second zone (Z2) is also accessible for reading and contains the results of encoding, using secret and public keys, of the data in the first memory zone.
Before the cardis sent to the user the first and third zones are written and the second zone data obtained by processing first and third zone data. When the card is read the **public key** is **validated** then the second zone data is computed and checked.
ADVANTAGE - Provides secure authentication of electronic memory cards which prevents fraudulent fabrication of cards from blank cards.
2/3
Title Terms: AUTHENTICITY; CARD; ELECTRONIC; MEMORY; THREE; ZONE; MEMORY; TWO; ZONE; READ; IMPLEMENT; TWO; LAYER; VALID; PROCESS
Derwent Class: T01; T04
International Patent Class (Additional): G06K-019/00; G07F-007/10; H04K-001/00
File Segment: EPI

5/5/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

004279566
WPI Acc No: 1985-106444/198518
XRPX Acc No: N85-079798
Blind signature systems for electronic banking - allows supplier to transform valid bank note message for digital signing then transform it back
Patent Assignee: SECURITY TECHNOLOGY CORP (SECU-N); CHAUM D (CHAU-I)
Inventor: CHAUM D
Number of Countries: 011 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 139313	A	19850502	EP 84201160	A	19840813	198518	B
US 4759063	A	19880719	US 83524896	A	19830822	198831	
EP 139313	B1	19920708	EP 84201160	A	19840813	199228	
DE 3485804	G	19920813	DE 3485804	A	19840813	199234	
			EP 84201160	A	19840813		

Priority Applications (No Type Date): US 83524896 A 19830822
Cited Patents: 3.Jnl.Ref; A3...8705; No-SR.Pub
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 139313	A	E	40		
	Designated States (Regional): AT BE CH DE FR GB IT LI NL SE				
EP 139313	B1	E	26	H04L-009/00	
	Designated States (Regional): AT BE CH DE FR GB IT LI NL SE				
DE 3485804	G			H04L-009/00	Based on patent EP 139313

Abstract (Basic): EP 139313 A

A first party (101) supplies messages to a second party (102) who returns to the first party a digital signature on supplied messages. A blind signal system is involved which includes generating a first secret key at the first party, this key being at least unknown to the second party. A message is transformed with the key and transmitted to the second party. A digital signature is formed of the transformed message with a secret signing key which is normally not known to the first party.

The digital signature is then transmitted from the second party to the first party. The digital signature is transformed at the first party with the first secret key to produce a second transformed message. The first and second transformed messages are not readily determined to correspond without knowledge of the first secrete key, and the second transformed message carries a digital signature properly relating to the message.

USE/ADVANTAGE - In banking using electronic money, without it being possible for the bank to trace all transactions validated by a customer's signature.

Title Terms: BLIND; SIGNATURE; SYSTEM; ELECTRONIC; BANK; ALLOW; SUPPLY; TRANSFORM; VALID; BANK; NOTE; MESSAGE; DIGITAL; SIGN; TRANSFORM; BACK
Derwent Class: W01
International Patent Class (Main): H04L-009/00
File Segment: EPI

```
Set     Items   Description
S1       2490   PUBLIC()KEY? ? OR KEYPAIR? OR PUBLICKEY?
S2         90   S1(3N)(SIGN OR SIGNS OR SIGNING OR SIGNED OR AGREEMENT? OR
               AGREE OR AGREE? ? OR RULE? OR VALIDAT? OR (LIMIT? OR CONTROL?-
               )()ACCESS?)
S3         80   S2 NOT PD=19940719:19970719
S4         60   S3 NOT PD=19970719:20000719
S5          3   S4 NOT PD=20000719:20031120
S6        548   S1(2N)(CONTROL? OR LIMIT? OR DENY OR PREVENT? OR HIDE? OR -
               SCRAMBLE? OR ENCRYPT? OR ENCIPHER? OR PROTECT?)
S7        497   S6 NOT PD=19940719:19970719
S8        380   S7 NOT PD=19970719:20000719
S9         19   S8 NOT PD=20000719:20031120
S10        19   S9 NOT S5
File 347:JAPIO Oct 1976-2003/Jul(Updated 031105)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200374
         (c) 2003  Thomson Derwent
```

10/5/18 (Item 14 from file: 350)
DIALOG(R)File 350:Derwent WPIX

004348531
WPI Acc No: 1985-175409/198529
Circuit cryptographic device - has microprocessor and digital signal processor which controls public key **forming operation NoAbstract Dwg 3/3**
Patent Assignee: FUJITSU LTD (FUIT)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 60105338	A	19850610	JP 83211712	A	19831112	198529	B

Priority Applications (No Type Date): JP 83211712 A 19831112
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 60105338	A		9		

Title Terms: CIRCUIT; CRYPTOGRAPHIC; DEVICE; MICROPROCESSOR; DIGITAL; SIGNAL; PROCESSOR; CONTROL; PUBLIC; KEY; FORMING; OPERATE; NOABSTRACT
Index Terms/Additional Words: SECRET; COMMUNICATE
Derwent Class: W01
International Patent Class (Additional): H04L-009/02
File Segment: EPI

```
Set     Items   Description
S1        562   PUBLIC()KEY? ? OR KEYPAIR? OR PUBLICKEY?
S2          6   S1(3N)(SIGN OR SIGNS OR SIGNING OR SIGNED OR AGREEMENT? OR
                 AGREE OR AGREE? ? OR RULE? OR VALIDAT? OR (LIMIT? OR CONTROL?-
                 )()ACCESS?)
S3         11   S1(2N)(CONTROL? OR LIMIT? OR DENY OR PREVENT? OR HIDE? OR -
                 SCRAMBLE? OR PROTECT?)
S4         17   S2 OR S3
S5          1   S4 NOT PY>1994
S6          1   S5 NOT PD>19940730
File 256:SoftBase:Reviews,Companies&Prods. 82-2003/Oct
         (c)2003 Info.Sources Inc
```

'6/3,K/1
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

01139424 DOCUMENT TYPE: Product

PRODUCT NAME: VeriTracks (139424)

General Dynamics Interactive (706639)
3190 Fairview Park Dr
Falls Church, VA 22042-4523 United States
TELEPHONE: (703) 876-3000

RECORD TYPE: Directory

CONTACT: Sales Department

REVISION DATE: 20030316

...extracts crime incident data from local law enforcement agencies' records management systems (RMSes). Information is **protected** with **public key** infrastructure (PKI) technologies. The Hit Engine component provides users with spatial analysis features, which can..

```
Set     Items   Description
S1       5761   PUBLIC()KEY? ? OR KEYPAIR? OR PUBLICKEY?
S2        752   S1(3N)(SIGN OR SIGNS OR SIGNING OR SIGNED OR AGREEMENT? OR
                 AGREE OR AGREE? ? OR RULE? OR VALIDAT? OR (LIMIT? OR CONTROL?-
                 )()ACCESS?)
S3        665   S2 NOT PD=19940719:19970719
S4        484   S3 NOT PD=19970719:20000719
S5         18   S4 NOT PD=20000719:20031120
S6       2706   S1(2N)(CONTROL? OR LIMIT? OR DENY OR PREVENT? OR HIDE? OR -
                 SCRAMBLE? OR ENCRYPT? OR ENCIPHER? OR PROTECT?)
S7       2458   S6 NOT PD=19940719:19970719
S8       1825   S7 NOT PD=19970719:20000719
S9         65   S8 NOT PD=20000719:20031120
S10        55   S9 NOT S5
S11        23   S10 NOT PUBLIC()KEY()(ENCIPHER? OR ENCRYPT?)
S12        41   S11 OR S5
File 348:EUROPEAN PATENTS 1978-2003/Nov W02
         (c) 2003 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20031113,UT=20031106
         (c) 2003 WIPO/Univentio
```

12/5,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00580551
STORAGE PROTECTION **UTILIZING** PUBLIC KEY CONTROL .
SPEICHERSCHUTZ MIT SCHUTZSCHLUSSEL.
PROTECTION DE MEMOIRE A L'AIDE D'UNE COMMANDE PAR CODES PUBLICS.
PATENT ASSIGNEE:
IBM DEUTSCHLAND GMBH, (276960), Pascalstrasse 100, D-70569 Stuttgart, (DE), (applicant designated states: DE)
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: CH;DK;ES;FR;GB;IT;LI;NL;SE;AT)
INVENTOR:
CLARK, Carl, Edward, 46 Bart Drive, Poughkeepsie, NY 12603, (US)
MALL, Michael Gerard, 53 La Crosse Drive, Morgan Hill, California 95037, (US)
SCALZI, Casper, Anthony, 16 Academy Street, Apt. 7E, Poughkeepsie, NY 12601, (US)
SINHA, Bhaskar, 19 Kendell Drive, Wappingers Falls, NY 12590, (US)
LEGAL REPRESENTATIVE:
Schafer, Wolfgang, Dipl.-Ing. (62021), IBM Deutschland Informationssysteme GmbH, Patentwesen und Urheberrecht, D-70548 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 587587 A1 940323 (Basic)
WO 9222032 921210
APPLICATION (CC, No, Date): EP 92909416 920429; WO 92EP926 920429
PRIORITY (CC, No, Date): US 710875 910606
DESIGNATED STATES: AT; CH; DE; DK; ES; FR; GB; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: G06F-012/14;
CITED PATENTS (WO A): FR 1562429 A; FR 1562429 A; US 4472790 A
CITED REFERENCES (WO A):
ELECTRO '86 AND MINI/MICRO NORTHEAST CONFERENCE RECORD November 1986, LOS ANGELES, US 21/2 pages 1 - 6; P. BUNCE ET AL.: 'System integrity in real-time MIL-STD-1750A environments';
NOTE:
No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	940323	A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	940323	A1	Date of filing of request for examination: 930903
*Assignee:	951102	A1	Applicant (transfer of rights) (change): IBM DEUTSCHLAND GMBH (276960) Pascalstrasse 100 D-70569 Stuttgart (DE) (applicant designated states: DE), International Business Machines Corporation (200120) Old Orchard Road Armonk, N.Y. 10504 (US) (applicant designated states: AT;CH;DE;DK;ES;FR;GB;IT;LI;NL;SE)
*Assignee:	960117	A1	Applicant (transfer of rights) (change): International Business Machines Corporation (200120) Old Orchard Road Armonk, N.Y. 10504 (US) (applicant designated states: AT;CH;DE;DK;ES;FR;GB;IT;LI;NL;SE)
*Assignee:	960117	A1	Previous applicant in case of transfer of rights (change): IBM DEUTSCHLAND GMBH (276960) Pascalstrasse 100 D-70569 Stuttgart (DE) (applicant designated states: DE)
Withdrawal:	980429	A1	Date on which the European patent application was deemed to be withdrawn: 971101

LANGUAGE (Publication,Procedural,Application): English; English; English

STORAGE PROTECTION **UTILIZING** PUBLIC KEY CONTROL .

12/5,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00527049
Public key cryptosystem key management based on control vectors.
Schlusselverwaltung fur Geheimubertragungssystem mit offentlichem Schlussel auf Grundlage von Steuervektoren.
Administration de cle pour systeme cryptographique a cle publique basee sur des vecteurs de commande.

PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: AT;CH;DE;DK;ES;FR;GB;IT;LI;NL;SE)
INVENTOR:
Matyas, Stephen M., 10 298 Cedar Ridge Drive, Manassas, VA 22 110, (US)
Johnson, Donald B., 11 635 Crystal Creek Lane, Manassas, VA 22 111, (US)
Le, An V., 10 227 Battlefield Drive, Manassas, VA 22 110, (US)
Prymak, Rostislaw, 15 900 Fairway Drive, Dumfries, VA 22 026, (US)
Martin, William C., 1835 Hilliard Lane, Concord, NC 28 025, (US)
Rohland, William S., 4234 Rotunda Road, Charlotte, NC 28 226, (US)
Wilkins, John D., P.O. Box 8, Somerville, VA 22 739, (US)
LEGAL REPRESENTATIVE:
Schafer, Wolfgang, Dipl.-Ing. (62021), IBM Deutschland Informationssysteme GmbH Patentwesen und Urheberrecht, D-70548 Stuttgart, (DE)

PATENT (CC, No, Kind, Date): EP 534419 A2 930331 (Basic)
EP 534419 A3 940629
APPLICATION (CC, No, Date): EP 92116307 920911;
PRIORITY (CC, No, Date): US 766260 910927
DESIGNATED STATES: AT; CH; DE; DK; ES; FR; GB; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: H04L-009/08;

ABSTRACT EP 534419 A2

A data processing system, method and program are disclosed, for managing a public key cryptographic system. The method includes the steps of generating a first public key and a first private key as a first pair in the data processing system, for use with a first public key algorithm and further generating a second public key and a second private key as a second pair in the data processing system, for use with a second public key algorithm. The method then continues by assigning a private control vector for the first private key and the second private key in the data processing system, for defining permitted uses for the first and second private keys. Then the method continues by forming a private key record which includes the first private key and the second private key in the data processing system, and encrypting the private key record under a first master key expression which is a function of the private control vector. The method then forms a private key token which includes the private control vector and the private key record, and stores the private key token in the data processing system.

At a later time, the method receives a first key use request in the data processing system, requiring the first public key algorithm. In response to this, the method continues by accessing the private key token in the data processing system and checking the private control vector to determine if the private key record contains a key having permitted uses which will satisfy the first request. The method then decrypts the private key record under the first master key expression in the data processing system and extracts the first private key from the private key record. The method selects the first public key algorithm in the data processing system for the first key use request and executes the first public key algorithm in the data processing system using the first private key to perform a cryptographic operation to satisfy the first key use request. (see image in original document)
ABSTRACT WORD COUNT: 343

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 930331 A2 Published application (A1with Search Report ;A2without Search Report)

Change:	930512	A2	Representative (change)
Examination:	930908	A2	Date of filing of request for examination: 930716
Change:	930929	A2	Representative (change)
Search Report:	940629	A3	Separate publication of the European or International search report
Change:	940921	A2	Representative (change)
Examination:	970611	A2	Date of despatch of first examination report: 970424
Withdrawal:	990602	A2	Date on which the European patent application was deemed to be withdrawn: 981215

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	3823
SPEC A	(English)	EPABF1	40413
Total word count - document A			44236
Total word count - document B			0
Total word count - documents A + B			44236

...SPECIFICATION specified as a parameter input to a cryptographic instruction, the PU authenticator is used to **validate** the **public key** as part of key recovery, before the recovered PU is processed within the cryptographic instruction...

...specified as a parameter input to a cryptographic instruction, the PR authenticator is used to **validate** the **public key** as part of key recovery, before the recovered PR is processed within the cryptographic instruction...length>0), or has no accompanying system signature (dsig1-length=0). If present, dsig1 is **validated** with a **public key** , PU, contained in the specified Internal Key Unit, IKU1. ePUM(keyblk) may be imported with...of the public key algorithm. The process of validating dsig consists of encryption with a **public key** , consistency checking to **validate** the redundancy bytes, and recovery of of the hash-value-of-reference originally used to...

12/5,K/9 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00291152
Controlling the use of cryptographic keys via generating station established control values.
Steuerung der Anwendung von Geheimubertragungsschlusseln durch in einer Erzeugungsstelle hergestellte Steuerwerte.
Commande de l'utilisation de cles cryptographiques par des valeurs de commande etablies dans une station de generation.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB;IT;NL)
INVENTOR:
Matyas, Stephen Michael, Jr., 8978 Miles Place, Manassa Virginia 22110, (US)
Meyer, Carl Heinz Wilhelm, 27 Norma Court, Kingston New York 12401, (US)
Brachtl, Bruno Oswald, Weinbergstrasse 20, D-7033 Herrenberg, (DE)
LEGAL REPRESENTATIVE:
Burt, Roger James, Dr. (52152), IBM United Kingdom Limited Intellectual Property Department Hursley Park, Winchester Hampshire SO21 2JN, (GB)
PATENT (CC, No, Kind, Date): EP 292790 A2 881130 (Basic)
EP 292790 A3 900124
EP 292790 B1 930818
APPLICATION (CC, No, Date): EP 88107596 880511;
PRIORITY (CC, No, Date): US 55502 870529
DESIGNATED STATES: DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS: H04L-009/00;
CITED PATENTS (EP A): US 4227253 A; US 4649233 A; US 4386233 A; US 4578530 A; WO 8102655 A

ABSTRACT EP 292790 A2
A method of controlling the use of securely transmitted information in a network of stations in which each potentially cooperating station includes a cryptographic facility (10) which securely stores a master key and in which, for each transmission between a pair of stations, a cryptographic key result is provided for each station of the pair by a generating station which is either one of the pair or a station external to the pair under a cryptographic protocol common to the network, the cryptographic key results for the transmission having a random component notionally particular to the transmission, a master key variant component characteristic of the protocol and a target station component either particular to the stations individually or as a pair, wherein, in response to a generating command invoked in the generating station for establishing a controlled use secure transmission between a designated pair of stations, the generating station generates the cryptographic key result for each designated station, accesses the control value common to the system for the permitted operation for each of the stations for the particular transmission, combines the control value with the common key result or each individual key result and causes the appropriate combined key result to be established in each station of the pair for the transmission, and wherein the cryptographic facility (10) in each station is arranged, when an operating command is invoked to perform a designated operation with respect to such securely transmitted information, to automatically abort such operation unless it matches the control value.

ABSTRACT WORD COUNT: 256

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 881130 A2 Published application (A1with Search Report ;A2without Search Report)
Examination: 890524 A2 Date of filing of request for examination: 890321
Search Report: 900124 A3 Separate publication of the European or International search report
Examination: 920401 A2 Date of despatch of first examination report: 920213

Change: 920722 A2 Representative (change)
Grant: 930818 B1 Granted patent
Change: 931006 B1 Representative (change)
Oppn None: 940810 B1 No opposition filed
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	4423
CLAIMS B	(German)	EPBBF1	2331
CLAIMS B	(French)	EPBBF1	2801
SPEC B	(English)	EPBBF1	15073
Total word count - document A			0
Total word count - document B			24628
Total word count - documents A + B			24628

...SPECIFICATION there is shown a data base 200 of encrypted keys, a data base 205 of **public values** , and a cryptographic facility 210 containing a command decoder 215, a random number generator 220...

...port 240 of the cryptographic facility 210. The encrypted transport key eKM(min) (KRi,j), **the public values** PVi and PVj, and the control values Ci and Cj are presented as data inputs...

12/5,K/12 (Item 12 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00254121
Cryptovariable initialisation in a public key network.
Voreinstellung einer Kryptovariablen in einem "Public Key"-Netz.
Initialisation d'une variable cryptographique dans un reseau a cle publique.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB;IT)
INVENTOR:
Matyas, Stephen Michael, 8978 Miles Place, Manassas, Virginia 22110, (US)
LEGAL REPRESENTATIVE:
Burt, Roger James, Dr. (52152), IBM United Kingdom Limited Intellectual Property Department Hursley Park, Winchester Hampshire SO21 2JN, (GB)
PATENT (CC, No, Kind, Date): EP 254812 A2 880203 (Basic)
EP 254812 A3 890927
EP 254812 B1 930127
APPLICATION (CC, No, Date): EP 87105550 870414;
PRIORITY (CC, No, Date): US 879784 860627
DESIGNATED STATES: DE; FR; GB; IT
INTERNATIONAL PATENT CLASS: H04L-009/08; H04L-009/30;
CITED PATENTS (EP A): EP 67977 A; EP 63794 A
CITED REFERENCES (EP A):
AFIPS CONFERENCE PROCEEDINGS, 1979 NATIONAL COMPUTER CONFERENCE, New York, 4th - 7th June 1979, vol. 48, pages 305-311, AFIPS Press, Montvale, US; E.H. MICHELMAN: "The design and operation of public-key cryptosystems"
IEEE COMMUNICATIONS MAGAZINE, vol. 23, no. 7, July 1985, pages 12-24, IEEE, New York, US; V.L. VOYDOCK et al.: "Security in high-level network protocols"
PROCEEDINGS OF CRYPTO '86, Santa Barbara, 11th - 15th August 1986, pages 451-458, Springer-Verlag, Berlin, DE; S.M. MATYAS: "Public key registration";

ABSTRACT EP 254812 A2
A procedure is disclosed for initialising with security and integrity a large number of terminals in an EFT/POS network with cryptographic variables. Each terminal in the network is provided with a terminal identification known to the key distribution centre, the public key of the key distribution centre is stored in the cryptographic facility of each terminal. A terminal initialiser is designated for each terminal, and the terminal initialiser for each terminal is notified of two expiration times for the purposes of registering the terminal's cryptovariable with the key distribution centre. The cryptovariable is generated by the terminal using its cryptographic facility. Prior to the first expiration time, a registration request is prepared and transmitted to the key distribution centre. The registration request includes the terminal identification and the cryptovariable. When the key distribution centre receives this request, the cryptovariable is temporarily registered and that fact is acknowledged to the requesting terminal. After the expiration of the second time, the registration is complete. Provisions are also made for invalidating a terminal identification in the event that more than one registration is attempted for a given terminal identification or that the registration was not made in time. The same procedure can be used to initialise cryptovariables of users of a network. The protocol is basically the same except that a user identification is used instead of a terminal identification, and the users may be provided with a transportable media, such as a magnetic stripe card or the like, which stores the user cryptovariable and can be read by terminals in the network.
ABSTRACT WORD COUNT: 264

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 880203 A2 Published application (A1with Search Report ;A2without Search Report)

Examination:	880629	A2	Date of filing of request for examination: 880426
Search Report:	890927	A3	Separate publication of the European or International search report
Examination:	911016	A2	Date of despatch of first examination report: 910830
Change:	920304	A2	Representative (change)
Grant:	930127	B1	Granted patent
Change:	931006	B1	Representative (change)
Oppn None:	940119	B1	No opposition filed
Lapse:	991020	B1	Date of lapse of European Patent in a contracting state (Country, date): IT 19930127,

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPABF1	609
SPEC B	(English)	EPABF1	8718
Total word count - document A			0
Total word count - document B			9327
Total word count - documents A + B			9327

...SPECIFICATION for each terminal;
FIGURE 2 is a time line diagram showing in graphical form the **rules** for the **public key** registration of a terminal in the system shown in Figure 1;
FIGURE 3 is a...

...1986, for T2. Denoting the date of receipt of the installation instructions as T0, the **rules** for the **public key** registration with respect to the expiration times T1 and T2 are shown in Figure 2...

12/5,K/28 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00255702 **Image available**
APPARATUS AND METHOD FOR PROVIDING NETWORK SECURITY
APPAREIL ET PROCEDE DE SECURISATION D'UN RESEAU
Patent Applicant/Assignee:
INTERNATIONAL STANDARD ELECTRIC CORP,
Inventor(s):
SNOW David A,
BOYLE John M,
MAIWALD Eric S,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9403859 A1 19940217
Application: WO 92US6369 19920731 (PCT/WO US9206369)
Priority Application: WO 92US6369 19920731
Designated States: CA JP AT BE CH DE DK ES FR GB GR IT LU MC NL SE
Main International Patent Class: G06F-013/14
International Patent Class: G06F-13:00; G06F-12:16
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6995

English Abstract
A multi-level security apparatus and method for a network employs a secure network interface unit (SNIU) coupled between each host or user computer unit (TS, S, S-U, PC, U) and a network, and a security manager (SM) coupled to the network, for controlling the operation and configuration of the SNIUs. Each SNIU is operative at a session level of interconnection which occurs when a user on the network is identified and a communication session is to commence. The SNIU is configured to perform a defined session level protocol, including the core function of user interface, session manager, dialog manager, association manager, data sealer, and network interface. The SM is implemented to ensure user accountability, configuration management, security administration, and validation key management on the network.

French Abstract
L'invention concerne un appareil et un procede de securite multiniveaux pour un reseau, qui utilisent une interface de reseau securisee couplee entre chaque ordinateur hote ou utilisateur (TS, S, S-U, PC, U) et un reseau, et un gestionnaire de securite (SM) couple au reseau permettant de controler le fonctionnement et la configuration des interfaces de reseau (SNIU). Chaque interface de reseau est active a un niveau session d'interconnexion qui survient lorsqu'un utilisateur du reseau est identifie et qu'une session de communication va commencer. L'interface de reseau est configuree pour executer un protocole defini de niveau session comprenant la fonction controle d'interface utilisateur, de gestionnaire de session, de gestionnaire de dialogue, de gestionnaire d'association, de classification de securite, et d'interface de reseau. Le gestionnaire de session est mis en oeuvre pour assurer la facturation de l'tuilisateur, la gestion de la configuration, l'administration de la securite, et la gestion des cles de validation sur le reseau.

Fulltext Availability:
Detailed Description

Detailed Description
... NSM). 'Me SSA exchanges
data and commands with its assigned SNIU, and performs initializatior4 configuration **control** , **access** controL **public key** management, audit/alarms, and other services for the SNIU. The ASM manages the security functions...in response to a NSM key request. The NSM returns a new certificate if the **public key** is **validated** . In addition, the NSM dictates when keys are to be generated by the SNITA. The...

12/5,K/29 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00247420 **Image available**
VERIFYING SECRET KEYS IN A PUBLIC-KEY CRYPTOSYSTEM
VERIFICATION DE CLEFS SECRETES DANS UN CRYPTOSYSTEME DE CLEFS PUBLIQUES
Patent Applicant/Assignee:
MICALI Silvio,
Inventor(s):
MICALI Silvio,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9321708 A1 19931028
Application: WO 93US3666 19930420 (PCT/WO US9303666)
Priority Application: US 92870395 19920420
Designated States: AU CA JP KR AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04K-001/00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 7600

English Abstract
A method, using a public-key cryptosystem, for enabling a predetermined entity (18) to monitor communications of users suspected of unlawful activities while protecting the privacy of law-abiding users, wherein each user is assigned a pair of matching secret and public keys. According to the method, each user's secret key is broken into shares. Then, each user provides a plurality of "trustees" (22a) pieces of information. The pieces of information provided to each trustee (22a) enable that trustee (22a) to verify that such information includes a "share" of a secret key of some given public key. Each trustee (22a) can verify that the pieces of information provided include a share of the secret key without interaction with any other trustee (22a) or by sending messages to the user. Upon a predetermined request or condition, e.g., a court order (20) authorizing the entity (18) to monitor the communications of a user suspected of unlawful activity, the trustees (22a) reveal to the entity (18) the shares of the secret key of such user. This enables the entity (18) to reconstruct the secret key and monitor the suspect user's communications.

French Abstract
Procede utilisant un cryptosysteme de clefs publiques, permettant a une entite predeterminee (18) de controler les communications d'utilisateurs suspectes d'activite illicite tout en protegeant le secret d'utilisateurs respecteux de la loi, dans lequel chaque utilisateur se voit attribue une paire de clefs secretre et publique assorties. Selon le procede, la clef secrete de chaque utilisateur est divisee en parts. Ensuite, chaque utilisateur fournit a une pluralite de "mandataires" (22a) des informations. Les informations fournies a chaque "mandataire" (22a) permettent a ce dernier de verifier que lesdites informations presentent une "part" de clef secrete d'une clef publique donnee. Chaque "mandataire" (22a) peut verifier que les informations fournies presentent une part de la clef secrete sans interaction avec aucun autre mandataire (22a), ou par transmission de messages a l'utilisateur. Lors d'une demande ou des conditions predeterminees, par exemple, un ordre de la cour (20) autorisant l'entite (18) a surveiller les communications d'un utilisateur soupconne d'activite illicite, les "mandataires" (22a) revelent a l'entite (18) les parts de ladite clef secrete de cet utilisateur. Ce procede permet a l'entite (18) de reconstituer la clef secrete et de surveiller les communications d'utilisateurs suspects.

Fulltext Availability:
Detailed Description

Detailed Description

... Each
trustee 22 individually inspects his received piece,
and, if it is correct, approves the **public key** (e.g.

signs it) and safely stores the piece relative to
it. These approvals are given to a...

...center 24, which may or may not coincide with the
government, itsiBlf approves: (e.g.,, **signs**) any **public**
key that is approved by all trustees, These
center-approved keys are the public keys of...degree of privacy of
communication offered
by the underlying Diffie-Hellman-scheme, in fact,
the **validation** of a **public key** does not compromise
the corresponding private key, Each trustee Ti
receives, as a special piece...

...own keys
and the pieces of his private one.

Second, if the key management center **validates**
the **public key** Px, then its private key is
guaranteed to be reconstructable by the government
in case...their piece of the private key, The encryption of
this piece -- in the trustee's **public key** and **signed**
by the trustee -- can be made part of the user's
public key. In this...

...electronic device, such as an
integrated circuit chip, the basic process of key
selection and **public - key validation** can be done
before the device leaves the factory, In this case,
it may be...

```
Set     Items   Description
S1       2767   (BOTH OR PUBLIC)()KEY? ? OR KEYPAIR? OR PUBLICKEY?
S2        350   S1(3N)(SIGN? OR AGREEMENT? OR AGREE OR AGREE? ? OR RULE? OR
                VALIDAT? OR (LIMIT? OR CONTROL?)()ACCESS?)
S3        283   S2 NOT AD=19940719:19970719
S4        213   S3 NOT AD=19970719:19990719
S5         91   S4 NOT AD=19990719:20010719
S6         50   S5 NOT AD=20010719:20031120
File 347:JAPIO Oct 1976-2003/Jul(Updated 031105)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200374
         (c) 2003  Thomson Derwent
```

6/5/1 **(Item 1 from file: 347)**
DIALOG(R)File 347:JAPIO

04969064 **Image available**
VERIFICATION METHOD FOR PROTECTING PRIVACY

PUB. NO.: 07-261664 [JP 7261664 A]
PUBLISHED: October 13, 1995 (19951013)
INVENTOR(s): FUJISAKI EIICHIRO
OKAMOTO TATSUAKI
OTA KAZUO
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 06-052323 [JP 9452323]
FILED: March 23, 1994 (19940323)
INTL CLASS: [6] G09C-001/00; H04L-009/22
JAPIO CLASS: 44.9 (COMMUNICATION -- Other); 44.3 (COMMUNICATION -- Telegraphy)

ABSTRACT

PURPOSE: To shorten the execution time in an verification method for protecting privacy by making it possible to check the authenticity of the electronic informa tion signed by a signer and making it impossible to collect the privacy informa tion of the signer therefrom.

CONSTITUTION: This verification method for protecting privacy consists of a center signature issuing process for having an authentified signature issued by a certificate issuing center VIC for the multiple **signature public key** of the tamper-free arithmetic unit OA given to the signer Alice from the certificate issuing center VIC and the signer Alice and a signature forming/verifying process for having the signature verified by the Verifier after the arithmetic unit OA and the signer Alice put the multiple signatures on a message. An RSA blind signing system is directly utilized at the time of issuing the center signature and the number of the multiplicands at the time of signature formation/ verification is decreased, by which the calculation quantity is curtailed.

```
Set     Items   Description
S1      13630   PUBLIC()KEY? ? OR KEYPAIR? OR PUBLICKEY?
S2        194   S1(3N)(SIGN OR SIGNS OR SIGNING OR SIGNED OR AGREEMENT? OR
                 AGREE OR AGREE? ? OR RULE? OR VALIDAT? OR (LIMIT? OR CONTROL?-
                 )()ACCESS?)
S3        230   S1(2N)(CONTROL? OR LIMIT? OR DENY OR PREVENT? OR HIDE? OR -
                 SCRAMBLE? OR PROTECT?)
S4        414   S2 OR S3
S5        342   RD (unique items)
S6         87   S5 NOT PY>1994
S7         87   S6 NOT PD=19940719:19970719
S8         87   S7 NOT PD=19970719:19990719
S9         87   S8 NOT PD=19990719:20010719
S10        87   S9 NOT PD=20010719:20031120
S11        86   S10 NOT CY>1994
S12        86   S11 NOT CD=19940719:19970719
S13        86   S12 NOT CD=19970719:19990719
S14        86   S13 NOT CD=19990719:20010719
S15        86   S14 NOT CD=20010719:20031120
File   8:Ei Compendex(R) 1970-2003/Nov W2
         (c) 2003 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2003/Oct
         (c) 2003 ProQuest Info&Learning
File  65:Inside Conferences 1993-2003/Nov W3
         (c) 2003 BLDSC all rts. reserv.
File   2:INSPEC 1969-2003/Nov W2
         (c) 2003 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2003/Nov W3
         (c)2003 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2003/Nov 14
         (c) 2003 The Gale Group
File 233:Internet & Personal Comp. Abs. 1981-2003/Jul
         (c) 2003, EBSCO Pub.
File   6:NTIS 1964-2003/Nov W3
         (c) 2003 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2003/Nov W2
         (c) 2003 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2003/Nov W3
         (c) 2003 Inst for Sci Info
File  62:SPIN(R) 1975-2003/Oct W1
         (c) 2003 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2003/Oct
         (c) 2003 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2003/Nov W1
         (c) 2003 FIZ TECHNIK
```

15/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04077982 E.I. No: EIP95022577638
Title: Authentication and protection **of** public keys
Author: Laih, Chi-Sung; Chiou, Wen-Hong; Chang, Chin-Chen
Corporate Source: Natl Cheng Kung Univ, Tainan, Taiwan
Source: Computers & Security v 13 n 7 1994. p 581-585
Publication Year: 1994
CODEN: CPSEDU ISSN: 0167-4048
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review); M; (Management Aspects)
Journal Announcement: 9504W4
Abstract: We propose a model, which is a hybrid of an ID-based scheme and a certificate-based scheme, to solve the authentication problem for users' public keys. Our model is used to improve the scheme presented by Girault at EUROCRYPTO '91. (Author abstract) 6 Refs.
Descriptors: *Security of data; Cryptography; File organization; Computer networks; Research and development management; Computer simulation; Security systems
Identifiers: ID based scheme; Certificate based scheme; Authentication; Public keys
Classification Codes:
723.2 (Data Processing); 723.5 (Computer Applications); 912.2 (Management); 714.1 (Electron Tubes)
723 (Computer Software); 912 (Industrial Engineering & Management); 714 (Electronic Components)
72 (COMPUTERS & DATA PROCESSING); 91 (ENGINEERING MANAGEMENT); 71 (ELECTRONICS & COMMUNICATIONS)

15/5/22 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

04195108 INSPEC Abstract Number: B9209-6120B-001, C9209-6130S-001
Title: The authenticability of public key protocols
Author(s): Tian Chang
Author Affiliation: Naval Submarine Coll., Qingdao, China
Journal: Chinese Journal of Computers vol.15, no.2 p.144-52
Publication Date: 1992 Country of Publication: China
CODEN: JIXUDT ISSN: 0254-4164
Language: Chinese Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: The paper considers the problems of **preventing** masquerade of **public key** protocols. An example of a protocol is analysed that cannot release a message but can bring about masquerade. A formal description of masquerade is given, and the formal definition of an authenticable protocol is proposed. The security (confidentiality and authenticability) of a practical protocol is proved. At last, an algorithm is presented with determines the authenticability of a given protocol. (9 Refs)
Subfile: B C
Descriptors: cryptography
Identifiers: authentication protocol; network security; protocol security ; public key protocols; formal description; masquerade; authenticable protocol; confidentiality
Class Codes: B6120B (Codes); C6130S (Data security)

15/5/74 (Item 34 from file: 144)
DIALOG(R)File 144:Pascal

06099844 PASCAL No.: 85-0361471
Encrypted broadcast communication using public master key
KOYAMA K
Journal: Review of the Electrical Communication Laboratories, 1984, 32 (5) 869-876
ISSN: 508535 Availability: CNRS-8413
No. of Refs.: 10 ref.
Document Type: P (Serial) ; A (Analytic)
Country of Publication: Japan
Language: English
On propose et on analyse, l'utilisation d'une cle d'acces generale, au lieu de plusieurs cles personnelles, pour le systeme du cryptographie de Rivest-Shamir-Adleman. On fournit une condition d'existence de cette cle generale, ainsi qu'un algorithme permettant de la calculer a partir des cles personnelles. Lors d'un protocole de diffusion secret, un emetteur code le message a l'aide de la cle generale publique, et les destinataires concernes le decodent a l'aide des cles personnelles secretes. La methode de la cle generale d'acces est superieure aux methodes anterieures

English Descriptors: Information **protection** ; Cryptography; **Public key** ; Broadcasting; Local network; System analysis
French Descriptors: Protection information; Cryptographie; Cle publique; Radiodiffusion; Reseau local; Analyse systeme; Cryptosysteme

15/5/31 (Item 11 from file: 2)
DIALOG(R)File 2:INSPEC

02427391 INSPEC Abstract Number: B85025033, C85020192
Title: Digital signature and cryptographic key management
Author(s): Koyama, K.
Author Affiliation: Musashino Electrical Communication Lab., NTT, Musashino, Japan
Journal: Information Processing Society of Japan vol.25, no.6 p. 554-60
Publication Date: 1984 Country of Publication: Japan
CODEN: JOSHA4 ISSN: 0447-8053
Language: Japanese Document Type: Journal Paper (JP)
Treatment: Applications (A); General, Review (G)
Abstract: Research on cryptography-based digital signatures is progressing. Research on the **protection** of **public keys** and signature keys is most important. This paper reviews recent research and practical applications of digital signatures and cryptographic-key management. The review centres around: (1) cryptography, (2) checking digital signatures, (3) generation of digital signatures and cryptographic keys, and (4) the distribution, installation and management of cryptographic keys. (23 Refs)
Subfile: B C
Descriptors: cryptography
Identifiers: cryptographic key management; digital signatures; protection ; public keys; signature keys; checking; distribution; installation
Class Codes: B6120B (Codes); C6130 (Data handling techniques)

15/5/18 (Item 18 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

01347842 E.I. Monthly No: EI8305032875 E.I. Yearly No: EI83021246
Title: PROTECTING PUBLIC KEYS **AND SIGNATURE KEYS.**
Author: Kenning, Dorothy E.
Corporate Source: Purdue Univ, West Lafayette, Indiana, USA
Source: Computer v 16 n 2 Feb 1983 p 27-35
Publication Year: 1983
CODEN: CPTRB4 ISSN: 0018-9162
Language: ENGLISH
Journal Announcement: 8305
Abstract: This article discusses the problem of protecting keys in a nationwide network using public-key cryptography for secrecy and digital signatures. Particular attention is given to detecting and recovering from key compromises, especially when a high level of security is required. 25 refs.
Descriptors: *CRYPTOGRAPHY; DATA PROCESSING--Security of Data
Classification Codes:
723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

```
Set     Items   Description
S1       2490   PUBLIC()KEY? ? OR KEYPAIR? OR PUBLICKEY?
S2         90   S1(3N)(SIGN OR SIGNS OR SIGNING OR SIGNED OR AGREEMENT? OR
               AGREE OR AGREE? ? OR RULE? OR VALIDAT? OR (LIMIT? OR CONTROL?-
               )()ACCESS?)
S3         44   S1(2N)(CONTROL? OR LIMIT? OR DENY OR PREVENT? OR HIDE? OR -
               SCRAMBLE? OR PROTECT?)
S4        113   SIGNATURE()KEY? ?
S5     673736   BROADCAST? OR MULTICAST? OR TELEVIS? OR TV? OR RADIO? OR C-
               ATV OR (BROAD OR MULTI)()CAST?
S6      76941   DIGITAL()SIGN?
S7       5408   S5(S)S6
S8         10   (S1 OR S4) AND S7
S9         24   (S1 OR S4) AND S5 AND S6
S10        21   S9 NOT AD=19940719:19960719
S11        15   S10 NOT AD=19960719:19980719
S12         7   S11 NOT AD=19980719:20010719
S13         4   S12 NOT AD=20010719:20031120
File 347:JAPIO Oct 1976-2003/Jul(Updated 031105)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200374
         (c) 2003  Thomson Derwent
```

13/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009333732 **Image available**
WPI Acc No: 1993-027195/199303
Related WPI Acc No: 1995-351022
XRPX Acc No: N93-020806

Robust data broadcasting **for e.g computer network of processor,storage units and printer - involves identifying originating node and including** digital signature **code word generated by encoding predetermined portions of transmission using private key**

Patent Assignee: DIGITAL EQUIP CORP (DIGI)
Inventor: PERLMAN R
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5175765	A	19921229	US 89349448	A	19890509	199303	B

Priority Applications (No Type Date): US 89349448 A 19890509
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5175765	A		18	H04L-009/30	

Abstract (Basic): US 5175765 A

In the **public - key** encryption system each node on the network is associated with a public and pivate key. A transmission over the network identifies its originating node and also includes a **digital - signature** code word generated by encoding predetermined portions of the transmission using the private key of the originating node.

When a transmission is received, the receiving node verifies that the transmission was originated by the identified originating node by manipulating the packet contents using the **public key** associated with the originating node. The packet is accepted only if the **digital - signature** code word in the packet corresponds to contents of the packet and the **public key** of the originating node.

ADVANTAGE - Reliably transmits packets over network subject to malicious failures.

Dwg.3/7

Title Terms: ROBUST; DATA; **BROADCAST** ; COMPUTER; NETWORK; PROCESSOR; STORAGE; UNIT; PRINT; IDENTIFY; ORIGIN; NODE; DIGITAL; SIGNATURE; CODE; WORD; GENERATE; ENCODE; PREDETERMINED; PORTION; TRANSMISSION; PRIVATE; KEY
Index Terms/Additional Words: ENCRYPTION
Derwent Class: W01
International Patent Class (Main): H04L-009/30
File Segment: EPI

Rogson 5,734,718

```
Set     Items   Description
S1      41659   PUBLIC()KEY? ? OR KEYPAIR? OR PUBLICKEY?
S2        859   S1(3N)(SIGN OR SIGNS OR SIGNING OR SIGNED OR AGREEMENT? OR
                 AGREE OR AGREE? ? OR RULE? OR VALIDAT? OR (LIMIT? OR CONTROL?-
                 )()ACCESS?)
S3        784   S1(2N)(CONTROL? OR LIMIT? OR DENY OR PREVENT? OR HIDE? OR -
                 SCRAMBLE? OR PROTECT?)
S4    4736850   (MULTICAST? OR BROADCAST? OR TELEVIS? OR CATV OR RADIO)
S5        261   SIGNATURE()KEY? ?
S6      34304   DIGITAL()SIGNATURE?
S7          0   S4(S)S5(S)S6
S8         22   S2(S)S3
S9          1   S8 NOT PY>1994
S10       240   S4(S)S6
S11        25   S1(S)S10
S12       270   (S2 OR S3)(S)S6
S13       293   S11 OR S12
S14        31   S13 NOT PY>1994
S15        27   S14 NOT PD=19940719:19960719
S16        27   S15 NOT PD=19960719:19990719
S17     16219   NONDISCLOSUR? OR NON()DISCLOSUR?
S18         3   S1(S)S17
S19      1325   (S2 OR S3) NOT (S13 OR S18)
S20       107   S19 NOT PY>1994
S21     44991   (CONFIDENT? OR SECREC? OR PRIVAC? OR PRIVAT?)(2N)(AGREEMEN-
                 T?)
S22         0   S21 AND S20
S23        98   S20 NOT PD=19940719:19960719
S24        98   S23 NOT PD=19960719:19980719
S25        98   S24 NOT PD=19980719:20000719
S26        98   S25 NOT PD=20000719:20030719
S27        47   S26 AND (AGREE? OR ACCEPT? OR S17 OR S5 OR APPROV? OR AFFI-
                 RM?)
File 275:Gale Group Computer DB(TM) 1983-2003/Nov 18
         (c) 2003 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2003/Nov 18
         (c) 2003 The Gale group
File  75:TGG Management Contents(R) 86-2003/Nov W2
         (c) 2003 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2003/Nov 18
         (c) 2003 The Gale Group
File  16:Gale Group PROMT(R) 1990-2003/Nov 18
         (c) 2003 The Gale Group
File 624:McGraw-Hill Publications 1985-2003/Nov 18
         (c) 2003 McGraw-Hill Co. Inc
File 484:Periodical Abs Plustext 1986-2003/Nov W3
         (c) 2003 ProQuest
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 239:Mathsci 1940-2003/Dec
         (c) 2003 American Mathematical Society
File 553:Wilson Bus. Abs. FullText 1982-2003/Oct
         (c) 2003 The HW Wilson Co
File 621:Gale Group New Prod.Annou.(R) 1985-2003/Nov 19
         (c) 2003 The Gale Group
File 674:Computer News Fulltext 1989-2003/Nov W2
         (c) 2003 IDG Communications
File  88:Gale Group Business A.R.T.S. 1976-2003/Nov 17
         (c) 2003 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 635:Business Dateline(R) 1985-2003/Nov 19
         (c) 2003 ProQuest Info&Learning
File  15:ABI/Inform(R) 1971-2003/Nov 19
         (c) 2003 ProQuest Info&Learning
File   9:Business & Industry(R) Jul/1994-2003/Nov 18
         (c) 2003 Resp. DB Svcs.
File 810:Business Wire 1986-1999/Feb 28
```

http://www.garlic.com/~lynn/secgloss.htm#t2269

public key

(I) The publicly-disclosable component of a pair of cryptographic keys used for asymmetric cryptography. (O) '(In a public key cryptosystem) that key of a user's key pair which is publicly known.' [**RFC2828**] A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and that may be made public. In an asymmetric (public) key cryptosystem that key of an entity's key pair that may be publicly known. A public key may be used to (1) verify a digital signature that is signed by the corresponding private key, (2) encrypt data that may be decrypted by the corresponding private key, and (3) compute a piece of shared information by other parties. The public key is used to verify a digital signature. This key is mathematically linked with a corresponding private key. [**SRV**] That key of an entity's asymmetric key pair which can be made public. [**SC27**] That key of an entity's asymmetric key pair which can be made public. NOTE - In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. **A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group. [SC27]** That key of an entity's asymmetric key pair which can be made public. [ISO/IEC FDIS 9796-2 (12/2001), ISO/IEC 11770-1: 1996, ISO/IEC WD 18033-1 (12/2001)] That key of an entity's asymmetric key pair which can be made public. NOTE - In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group. [**SC27**] The key in a matched key pair - private key and public key - that may be published, e.g. posted in a directory, for public key cryptography. [**AJP**] The key in a matched key pair-private key and public key - that is made public; for example, posted in a public directory for public key cryptography. [**SRV**] (see also asymmetric algorithm, cryptography, key, public-key infrastructure)

Information from SC27 site ISO SubCommittee 27....

public key

That key of an entity's asymmetric key pair which can be made public. [ISO/IEC FDIS 9796-2 (12/2001), ISO/IEC 11770-1: 1996, ISO/IEC WD 18033-1 (12/2001)]

That key of an entity's asymmetric key pair which can be made public.

NOTE - In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-3: 1999, ISO/IEC WD 13888-1 (11/2001), ISO/IEC FDIS 15946-3 (02/2001)]

ISO/IEC DIS 11770-3.2: 1997

Information technology - Security techniques -

Key management - *Part 3: Mechanisms using asymmetric techniques*

1. **Project reference:** JTC 1.27.18.03
2. **Responsible WG:** JTC 1/SC 27/WG 2
3. **Scope**

   This part of ISO/IEC 11770 defines key management mechanisms based on asymmetric cryptographic techniques. Some of the mechanisms of this part of ISO/IEC 11770 are based on the corresponding authentication mechanisms in ISO/IEC 9798-3.

   This part of ISO/IEC 11770 does not cover aspects of key management such as key lifecycle management and mechanisms to store, archive, delete, destruct, etc. keys. It also does not cover the implementations of the transformations used in the key management mechanisms.

4. **Abstract of objectives**

   This part of ISO/IEC 11770 specifically addresses the use of asymmetric techniques to achieve the following goals:

   - Establish a shared secret key between two entities A and B by key agreement. In a secret key agreement mechanism the secret key is the result of a data exchange between the two entities A and B. Neither of them can predetermine the value of the shared key.
   - Establish a shared secret key between two entities A and B by key transport. In a secret key transport mechanism the secret key is chosen by one entity A and is transferred to another entity B, suitably protected by asymmetric techniques.
   - Make an entity's public key available to other entities by key transport. In a public key transport mechanism, the public key of an entity A must be transferred to other entities in an authenticated way, but not requiring secrecy.

5. **Dependencies**

   This document is part of a multi-part standard. Some mechanisms make use of the techniques specified in ISO/IEC 9798-3, Entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm.

6. **History/Target dates**

   CD 1993
   (FDIS 1998-05)
   (IS 1998-11)